Comments—NBP Public Notice #17
GN Docket Nos. 09-47, 09-51, 09-137; and WC Docket No. 02-60.

December 4, 2009

Julius Genachowski
Chairman of the Federal Communications Commission
c/o Marlene Dortch
Office of the Secretary
Federal Communications Commission

Dear Mr. Genachowski:

The Center for Democracy and Technology (CDT), through its Health Privacy Project, promotes comprehensive policies to protect the privacy and security of health information as it is increasingly exchanged through the use of information technology. CDT submits this letter in response to the Federal Communications Commission (FCC) call for Comments on Health Care Delivery Elements of a National Broadband Plan (NBP Notice #17). This letter addresses Section 5, "Data Security in Health IT," part d, which asks how to simplify the means by which patients obtain their medical information and populate Personal Health Records (PHRs).

CDT supports the inclusion of ways for consumers to more easily obtain their health information and populate PHRs in the FCC National Broadband Plan. But, in doing so, CDT urges the FCC to be aware of and provide support for baseline privacy and security protections for health information in commercial PHRs.

Health information technology (HIT) and electronic health information exchange have the potential to improve health care quality and efficiency, while also empowering consumers to play a greater role in their own care. A large majority of the public wants electronic access to their personal health information because they believe such access is likely to increase their quality of care. At the same time, however, the public is very concerned about the privacy and security risks that health IT poses. Fostering trust in health IT systems is pivotal to fully realizing the benefits of technology and is best achieved through enhanced privacy and security built into health IT systems. The latter will bolster consumer trust and confidence and initiate the rapid adoption of health IT and the realization of its benefits.

This is particularly true in the case of Personal Health Records (PHRs). PHRs hold significant potential for consumers to become key, informed decision-makers in their own (or a family member's) health care. PHRs can be drivers of needed change in our health care system by providing consumers with options for storing and sharing copies of their health records, as well

as options for recording, storing, and sharing other information that is often relevant to health care but is often absent from official medical records. But for consumers to feel comfortable using PHRs, they need assurance that their information will be protected by reasonable privacy and security safeguards.

Consumer concern over using PHRs is justified. Currently, there are no consistent rules protecting health information stored in and shared from PHRs, and there are arguably no national privacy and security standards governing PHRs provided by entities outside the coverage of the Health Insurance Portability and Accountability Act (HIPAA). When physicians, hospitals, and health plans offer PHRs, the HIPAA privacy and security regulations apply. However, when commercial entities or employers provide PHRs, or when information from PHRs is shared with an outside entity such as through a third-party application or social networking site, no substantive privacy and security standards apply except that the company must comply with any privacy policy it elects to create.

It seems intuitive to suggest then that HIPAA privacy and security regulations be extended to protect health information in PHRs as well. But HIPAA was drafted to address the privacy and security issues raised by traditional health care records, not consumer-driven PHRs. As such, the broad application of HIPAA could actually make health information less safe in the PHR space because it permits a number of disclosures without consumer consent for treatment, payment, or healthcare operations. To add, HIPAA's exclusive reliance on consumer authorization to protect consumers against inappropriate commercial use of their information is inadequate.

Consumers using PHRs should instead be protected by a comprehensive privacy and security framework that targets the risks to consumers using them; is flexible enough to allow for innovation to meet a wide array of consumer needs; and that covers both the PHR vendor or provider as well as third-party applications or business partners that consumers allow to access information in the PHR. [1] The Administration has an opportunity to make progress in addressing this issue, as the U.S. Department of Health and Human Services (HHS) (working with the Federal Trade Commission (FTC)) is required to recommend privacy and security protections for PHRs not covered by HIPAA (as part of The American Recovery and Reinvestment Act of 2009 (ARRA). A report is due to Congress with the agencies' recommendations no later than February 18, 2010. The report must also recommend which agency should regulate PHRs and entities that access health information through PHRs going forward. However, Congress stopped short of requiring the actual promulgation of regulations. Support from the FCC for a comprehensive framework of rules protecting information in PHRs will be important to ensuring that such a framework is enacted into law.

Of note, ARRA did impose breach notification requirements that apply to PHRs (and certain third-party applications), which went into effect September 23, 2009. HHS has issued regulations to govern notification by those PHRs covered by HIPAA, [2] and FTC has issued

---

[1] See http://www.cdt.org/testimony/testimony-deven-mcgraw-ncvhs for more details on CDT's preliminary recommendations on how to protect consumers using PHRs.

[2] See HHS Interim Final Rule on Breach Notification for Unsecured Protected Health Information (August 24, 2009), at http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf.

regulations to govern notification by any PHRs not covered by HIPAA.[3] Both sets of requirements include a safe harbor that CDT hopes will encourage all PHR providers to adopt strong security safeguards, including encryption. Specifically, notification is not required if the information that was breached was rendered inaccessible, unusable or indecipherable using a technology or methodology adopted by HHS in annual Guidance. HHS Guidance currently includes only strong data encryption and destruction standards.[4] Although PHR providers and third-party applications are not required to adopt these strong security safeguards, they have a strong incentive to do so in order to avoid breach notification. CDT supports the safe harbor approach and the HHS Guidance as a critical first step to securing adequate security safeguards to protect individuals using PHRs.

CDT appreciates the opportunity to provide comments to the FCC on the Health Care Delivery Elements of a National Broadband Plan. Please let us know if you have any questions or need further information.

Sincerely,

//Deven McGraw

Deven McGraw
Director, Health Privacy Project

[3] See FTC Final Rule on Health Breach Notification (August 25, 2009), at http://www.ftc.gov/os/2009/08/R911002hbn.pdf.

[4] See HHS Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements under the American Recovery and Reinvestment Act of 2009, at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf.